511, 934

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 November 2003 (06.11.2003)

PCT

(10) International Publication Number
WO 03/092215 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/FI03/00282

(22) International Filing Date: 14 April 2003 (14.04.2003)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data:
20025018 23 April 2002 (23.04.2002) FI

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 ESPOO (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **AHONEN, Petri** [FI/FI]; Hetteikkö 5, FIN-40250 JYVÄSKYLÄ (FI).

(74) Agent: **KESPAT OY**; P.O.Box 601, FIN-40101 JYVÄSKYLÄ (FI).

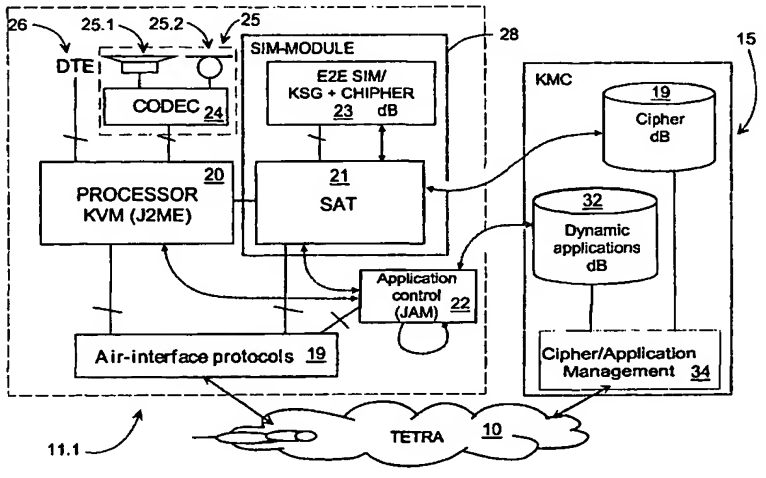
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM IN A DIGITAL WIRELESS DATA COMMUNICATION NETWORK FOR ARRANGING END-TO-END ENCRYPTION AND CORRESPONDING TERMINAL EQUIPMENT



(57) Abstract: The invention concerns a system in a digital wireless data communication network (10) for arranging end-to-end (e2e) encryption, especially for communication in audio form in which the data communication network (10) two or more pieces of terminal equipment (11.1, 11.2) are communicating with one another, including at least - a codec (24) for converting an analog audio signal into a dataflow and vice versa, - air-interface encryption means (19, 30), - means (28) for management of encryption parameters (TEK, IV) stored in connection with the terminal equipment (11.1, 11.2) - an encryption key stream generator KSG (23) to generate an key stream segment (KSS) with the said encryption parameters (TEK, IV), - means (20) for encrypting a dataflow and for decrypting the encryption with the generated key stream segment (KSS, IV), - means (33.1, 33.2) for synchronization of the encrypted dataflow and for de-synchronizing the synchronization, and - at least one interface (19) for receiving encryption parameters from the data communication network (10), and wherein at least one of the pieces of terminal equipment belonging to the data communication network (10) is adapted to function as a special server terminal device (15), which manages and distributes at least encryption parameters (19) concerning the data communication network (10) to the other pieces of terminal equipment (11.1, 11.2) based on an established criterion. In the data communication network (10) a said special server terminal device (15) is also arranged to manage at least encryption and/or synchronization applications (32) and to distribute these according to an established criterion to the other pieces of terminal equipment (11.1, 11.2), and - in the terminal equipment (11.1, 11.2) are arranged functionalities (21, 22) for downloading and managing the said applications (32) as well as - data memory (23) for saving applications (32) and - a processor (20) and operating memory for carrying out applications (32).

WO 03/092215 A1